1. PURPOSE

The NMCI employs a defense-in-depth approach to information assurance that requires diligence and vigilance on the part of all users and operators. The operation and use of the system with respect to protection of information and system resources is bound by a set of information security policies Passwords are a key element in the defense-in-depth approach and provide protection from direct access to systems by unauthorized individuals.

2. POLICY

2.1 USER ACCOUNTS

Passwords are required for all user accounts within the NMCI. User accounts are defined as those accounts that are provided to the customer community users or to the members of the NMCI ISF team. Government user accounts consist of specific accounts that are bound to specific individuals, generic accounts that are bound to a specific location, and functional accounts that are bound to a specific location and a group Access Control List (ACL). These accounts have limited rights and have a defined set of applications and data access.

2.1.1 DEFAULT PASSWORDS

Default passwords do not meet ISF and Navy security policies. A default password is one that was provided to a user by ISF during transition. ISF will lockout any account that has a known identified default password. Users should replace any ISF-provided passwords with unique, strong passwords described in the tables below. If a user continues to access the network using a default password the account will be locked and the user must call the helpdesk to get the account unlocked (with a new, strong password). Customer data files and mail will not be lost when the account is locked out and will be available to the user once the password is changed.

2.2 INFRASTRUCTURE ADMINISTRATION ACCOUNTS [OTHER THAN INFORMATION ASSURANCE (IA)]

Passwords are required for all infrastructure administration accounts within the NMCI. Infrastructure administration accounts are utilized by the network operations staff to access controlled assets of the NMCI for a variety of reasons. These accounts include the administrator accounts on all assets (desktops, routers, switches, etc.) and all infrastructure functional accounts. The administrator accounts have full system access and are controlled accordingly. The infrastructure functional accounts have a significant impact on NMCI availability and are controlled accordingly.

2.3 INFORMATION ASSURANCE INFRASTRUCTURE ASSETS

Passwords are required for all Information Assurance accounts within the NMCI. IA assets consist of the set of platforms and tools that are used by the IA organization to protect and monitor the NMCI for potential penetration or exploit attempts. These accounts may have either

limited or full system access rights but are protected separately due to their protection and monitoring function.

2.4 UNCLASSIFIED NMCI POLICY APPLICATION

Area	User Account	Infrastructure Administration Account	IA Asset Administration Account
Vendor Default Password	Reset by Account Holder on install	Reset by Account Holder on install	Reset by Account Holder on install
Install Default Password	Reset by Account Holder on initial access	Reset by Account Holder on install	Reset by Account Holder on install
Account Holder	Asset user	Specific Network Operations Center (NOC) Analyst	Specific Global Information Assurance Center (GIAC) Analyst
Password Reset Life	Not more than 90 days	Not more than 90 days	Not more than 90 days
Password Disclosure	None	By owner according to disclosure policy	By owner according to disclosure policy
Password Strength • Length	Not less than 8 characters	Not less than 8 characters	Not less than 8 characters
• Capitals, Lower Case, Numbers, Special Characters	Must include at least 2 character types	Must include one of each character type	Must include at least 2 of each character type
• Common Names	Allowed but discouraged	Not allowed	Not allowed
• Password Offline Storage	Allowed but discouraged	Password log in local vault under access control	Password log in local vault under access control
Password Network Storage	Not allowed	Not allowed	Not allowed
Password Evaluation by Information Assurance	Randomly	At least quarterly	On reset
Password Evaluation Failure Action	Reset to random	Notification to Global Network Operations Center (GNOC) Manager	Notification to GIAC Manager
Password Reset Authority	Account Holder	Regional Network Operations Center (RNOC) Manager	Regional Information Assurance Center (RIAC) Manager

2.5 CLASSIFIED NMCI POLICY APPLICATION

Area	User Account	Infrastructure Administration Account	IA Asset Administration Account
Vendor Default Password	Reset by Account Holder on install	Reset by Account Holder on install	Reset by Account Holder on install
Install Default Password	Reset by Account Holder on initial access	Reset by Account Holder on install	Reset by Account Holder on install
Account Holder	Asset user	Specific NOC Analyst	Specific GIAC Analyst
Password Reset Life	Not more than 90 days	Not more than 90 days	Not more than 90 days
Password Disclosure	None	By owner according to disclosure policy	By owner according to disclosure policy
Password Strength • Length	Not less than 8 characters	Not less than 8 characters	Not less than 8 characters
• Capitals, Lowercase, Numbers, Special Characters	Must include at least two character types	Must include one of each character type	Must include at least 2 of each character type
• Common Names	Not Allowed	Not Allowed	Not Allowed
• Password Offline Storage	Not Allowed	Password log in local vault under access control	Password log in local vault under access control
Password Network Storage	Not allowed	Not allowed	Not allowed
Password Evaluation by Information Assurance	Randomly	At least quarterly	On reset
Password Evaluation Failure Action	Reset to random	Notification to GNOC Manager	Notification to GIAC Manager
Password Reset Authority	Account Holder	RNOC Manager	RIAC Manager

3. IMPLICATIONS

Title	Description
Global Information Assurance Center Manager (GIAC)	Responsible for establishment, promulgation, modification and enforcement of policy.

Title	Description
Global Network Operations Center Manager (GNOC)	Responsible for review, promulgation, modification, and enforcement of policy.
Regional Information Assurance Center Manager (RIAC)	Responsible for carrying out the established policy using sound processes and procedures.
Regional Network Operations Center Manager (RNOC)	Responsible for carrying out the established policy using sound processes and procedures.
ISF Site Managers	Responsible for carrying out the established policy using sound processes and procedures.
ISF Quality Assurance	Responsible for audit of operational system to determine compliance to established policy and supporting processes and procedures.
ISF Configuration Management	Responsible for controlled change activity to the NMCI system.
Information System Security Administrator (ISSA)/Regional Information System Security Administrator (RISSA)	Coordinates with the S-ISSM and/or the site Commanding Officer for site related INFOSEC issues and interfaces with the RNOC ISSC for items escalated to the RNOC. Coordinates with the RIAC for site configuration and risk mitigation actions.
IA Operations Director	Information Assurance professional responsible for all IA operational activities on the NMCI. Contact interface to EDS for reporting and response.

4. DEFINITIONS AND ACRONYMS

Term	Definition
Alarm	Indication by an IA countermeasure that an abnormal activity has occurred
Alarm of Interest -- AOI	An alarm that has been evaluated by an IA professional and is deemed to be either a known threat action or an unknown action that requires further analysis
ACL	Access Control List
ATO	Ongoing approval to operate a network as part of an approved Government network. Status after clearance of IATO discrepancies
C&A	Certification and Accreditation – Certification is technical identification of vulnerabilities while accreditation is assessment of risk and willingness to accept. Risk may be accepted with restrictive caveats – Includes IATC, IATO, and ATO
CNNSOC	Commander of Naval Network Systems Operations Command
DITSCAP	Defense Information Technology Systems Certification and Accreditation Program
ECCB	Enterprise Change Control Board
Event	An evaluated alarm of interest that meets the conditions of a potential penetration attempt or other suspicious activity
Event of Interest -- EOI	An event that has been evaluated as an actual successful penetration attempt or other successful IA system service interruption

Term	Definition
GIAC	Global Information Assurance Center
GNOC	Global Network Operations Center
Help Desk Incident	An issue reported by an NMCI end user. May or may not be an IA event.
IA Incident	A PI that has been determined by CNNOC to be an actual incident – Requires in-depth reporting
IATC	Interim Authority to Connect – Approval by the Government to connect a network to an approved Government network
IATO	Interim Authority to Operate – Approval by the Government to operate a network as part of an approved Government network
IAVA	Information Assurance Vulnerability Alert – Government defined alarm on a particular threat – Action and Reporting required
IAVB	Information Assurance Vulnerability Bulletin – Government defined advisory on a particular threat – Reporting not required
IDS	Intrusion Detection System
INFOCON	Information Condition
ISSA	Information System Security Administrator – ISF site representative for issues related to Information Security (INFOSEC)
RISSA	Regional Information System Security Administrator -- ISSA responsible for multiple sites within the NMCI
ISSC	Information System Security Coordinator -- USN or USMC RNOC/GNOC representative for issues related to Information Security (INFOSEC). Coordinates INFOSEC issues with ISSA/RISSA.
S-ISSM	Site - Information System Security Manager – USN or USMC site representative for issues related to Information Security (INFOSEC)
ITA	Symantec Intruder Alert – A host based IDS
NISPOM	National Industrial Security Program Operating Manual
Policy	A statement of management philosophy approved by NMCI senior executives. Policy documents may define implementation instructions, authority delegations, or other actions needed to meet requirements.
PC	Performance Category – Subset of performance required for a particular SLA
Potential Incident -- PI	Events of interest that have been evaluated to meet the criteria of an actual targeted service interruption – Elevated to CNNOC for evaluation of an actual Incident
RFC	Request for change – Nomination of a change for incorporation in the NMCI architecture or work methods.
RIAC	Regional Information Assurance Center
RNOC	Regional Network Operations Center
SSAA	System Security Authorization Agreement
SLA	Service Level Agreement

5. DOCUMENT CHANGE HISTORY

(List in Reverse Chronological Order)

Effective	Version	Explain the Change Action	By	CAD No.
<YR.MTH.DY>	<0.00>	Initial Release		

6. DOCUMENT REVIEW HISTORY

(List in Reverse Chronological Order)

Reviewed	By	Reason	Results	Comments	CAD No.
<YR.MTH.DY>					

7. DOCUMENT CONTROL INFORMATION

Document ID	Document Owner Team Lead	Document Approver Team Lead	Stored	Retention	Disposition
ES.EP.00.000.19.000.F+0	P. Mermagen	NMCI Service Delivery Manager	ISF Ops Library	Until No Longer Valid	N/A